IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Steven G. Fry, Shantanu Sarkar		
Assignee:	Cisco Technology, Inc.		
Title:	Method And Apparatus Supporting Network Communications Through A Firewall		
Serial No.:	09/456,692	Filed:	December 9, 1999
Examiner:	Carl G. Colin	Group Art Unit:	2136
Docket No.:	CIS0044US	Client Ref. No.:	1669

Austin, Texas
November 27, 2006

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 CFR § 41.37

Dear Sir:

This brief is submitted in support of the appeal filed herewith by the appellants to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 107-147 and 165-181. Filed herewith is a Petition for Extension of Time requesting a two-month extension, thereby giving the undersigned a period until November 27, 2006 (November 26, 2006 being a Saturday) in which to respond.

Please charge deposit account No. 502306 for the fee of $500.00 associated with this appeal brief. Please charge this deposit account for any additional sums which may be required to be paid as part of this appeal.

REAL PARTY IN INTEREST

The real party in interest on this appeal is Cisco Technology, Inc.

RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences related to this application.

STATUS OF CLAIMS

Claims 107, 125, 131, 145, 165, 179, "and the intervening claims" (*See* Final Office Action of June 26, 2006, p. 5, ¶1) are rejected under 35 U.S.C §112, first paragraph. Claims 107-127 and 131-148 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U. S. Patent 5,941,988 issued to Bhagwat et al. ("Bhagwat"). Claims 165-181 also appear to be rejected under 35 U.S.C. § 102(e) as being anticipated by Bhagwat (*See* Final Office Action of June 26, 2006, p. 12, ¶3, and p. 13, ¶1). Claims 128-130 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bhagwat in view of U. S. Patent 6,104,716 issued to Chrichton *et al.* ("Chrichton"). Claims 107-147 and 165-181 are being appealed.

STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection of June 26, 2006.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention is as set forth in the claims. To summarize the invention without intending to limit or otherwise affect the scope of the claims, the invention as set forth by independent claim 107 relates to a method. A plurality of sockets are provided. See, for example, the list of currently open sockets described on p. 12, lines 1-3 of the specification, and Figure 4. Each socket has an associated connection and an associated security token, and the associated security token is provided by the associated connection. See, for example, p. 11, line 22 through p. 12, line 7 of the specification. A first connection and a first security token are received. See, for example, p. 12, lines 1-15, and other description associated with Figure 4. A socket associated with the first connection is created. The first connection has associated the first security token. See, for example, operation 400 of Figure 4 and p. 11, lines 19-30. The first security token is compared with the associated security tokens. See, for example, operations 420 and 430 of Figure 4, and p. 12, lines 1-19. In response to the comparing, the socket is included in the plurality of sockets if none of the associated security tokens match the first security token. See, for example, operation 470 of Figure 4 and p. 12, lines 12-25.

The invention is further set forth by independent claim 120 which relates to a method. A first connection to a first program is created. See, for example, operation 300 of Figure 3, and p. 10, lines 6-27. A first security token is received from the first program. See, for example, p. 10, lines 1-5, and p. 12, lines 1-11. A second connection is created to a relay program. See, for example, operation 320 of Figure 3. The first security token is provided to the relay program. See, for example, p. 12, lines 1-11. Upon successful creation of the second connection, the first connection is coupled to the second connection. See, for example, operation 340 of Figure 3.

The invention as set forth by independent claim 131 relates to an apparatus. Note that the various computer systems and software for implementing the functions of claim 131 are shown, for example, in Figure 2 and described on p. 10, line 28 through p. 11, line 8. A plurality of sockets are provided, for example, by a list maintained by relay program 210 which operates on computer system 220. See, for example, the list of currently open sockets described on p. 12, lines 1-3 of the specification, and Figure 4. Each socket has an associated connection and an associated security token, and the associated security token is provided by the associated connection. See, for example, p. 11, line 22 through p. 12, line 7 of the specification. The apparatus also includes a means for receiving a first connection and a first security token. Again, relay program 210 operating on computer system 220 is an example of such a means. See, for example, p. 12, lines 1-15, and other description associated with Figure 4. A means for creating a socket associated with the first connection (e.g., program/system 210/220) is also included. The first connection has associated the first security token. See, for example, operation 400 of Figure 4 and p. 11, lines 19-30. The apparatus also includes a means for comparing the first security token with the associated security tokens (210/220). See, for example, operations 420 and 430 of Figure 4, and p. 12, lines 1-19. In response to the comparing, the socket is included in the plurality of sockets if none of the associated security tokens match the first security token. See, for example, operation 470 of Figure 4 and p. 12, lines 12-25.

The invention as set forth by independent claim 140 relates to an apparatus. Note that the various computer systems and software for implementing the functions of claim 131 are shown, for example, in Figure 2 and described on p. 10, line 28 through p. 11, line 8. The apparatus includes a means for creating a first connection to a first program, for example, protocol daemon 250 operating on computer system 105. See, also, operation 300 of Figure 3, and p. 10, lines 6-27. Daemon 250/system 105 is also an example of a means for receiving a first security token from the first program. See, also, p. 10, lines 1-5, and p. 12, lines 1-11. Daemon 250/system 105 is also an example of a means for creating a second connection is a relay program. See, also, operation 320 of Figure 3. The apparatus also includes a means for providing first security token to the relay program, e.g., daemon 250/system 105. There is also a means for the first connection to the coupling the second connection upon successful creation of the second connection, e.g., daemon 250/system 105. See, also, operation 340 of Figure 3.

The invention as set forth by independent claim 165 relates to a computer program product. Note that software for implementing the functions of claim 165 are shown, for example, in Figure 2 and described on p. 10, line 28 through p. 11, line 8. Otherwise, claim 165 can be summarized as claim 107 above.

The invention as set forth by independent claim 174 relates to a computer program product. Note that software for implementing the functions of claim 165 are shown, for example, in Figure 2 and described on p. 10, line 28 through p. 11, line 8. Otherwise, claim 174 can be summarized as claim 120 above.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claims 107-119, 131-139, and 165-173 are rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement.

II. Claims 125-127, 145-147, and 179-181 are rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement.

III. Claims 107-119, 131-139, and 165-173 stand rejected under 35 U.S.C. § 102(e) (either directly or via a rejected parent claim) as being anticipated by U. S. Patent 5,941,988 issued to Bhagwat et al.

IV. Claims 120-130, 140-147, and 174-181 stand rejected under 35 U.S.C. § 102(e) (either directly or via a rejected parent claim) as being anticipated by U. S. Patent 5,941,988 issued to Bhagwat et al.

ARGUMENT

35 U.S.C. § 112, First Paragraph – Claims 107-119, 131-139, and 165-173

Claims 107, 131, and 165 are explicitly rejected under 35 U.S.C §112, first paragraph. The claims depending from those independent claims also appear to be similarly rejected. *See* Final Office Action of June 26, 2006, p. 5, ¶1. The appellants present an argument with respect to independent claim 107, as the relevant limitations in independent claims 131 and 165 are generally the same as those in claim 107. Further, claims 108-119, 132-139, and 166-173 depend from independent claims 107, 131, and 165, respectively.

The Examiner rejects these claims as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors(s), at the time the application was filed, had possession of the claimed invention. In particular, the Examiner states:

> At the time the invention was made, Applicant was not concerned of having the invention implemented in a network concept of socket as disclosed in the claims. The plurality of sockets claimed by the applicant in the last action, as interpreted by the Examiner, represented the socket of the first connection and the matching socket. Given the claims now as amended, it appears that Applicant is referring to the list of currently open sockets (to be searched for match), because Applicant now claims that the socket (interpreted as the attempted connection) is included in the plurality of sockets in response to no match. Therefore, the specification does not describe, "providing a plurality of sockets, wherein each socket has an associated connection and an associated security token and the associated security token is provided by the associated connection". The disclosure does not even explicitly states, "the socket" is included in the plurality of sockets. In addition, the disclosure does not describe, "creating a socket associated with the first connection wherein the first connection has associated the first security token." The disclosure merely states "create a socket for use by an inbound connection" this socket was never mentioned afterwards, and merely states "a password is provided". The association that Applicant is claiming with the created socket having an associated connection and associated token is not explicitly disclosed. (Final Office Action of June 26, 2006, p. 5, ¶1 through p. 6, top)

The appellants respectfully disagree, and for the sake of clarity respond to each of the Examiner's points in succession.

First, the Examiner argues the appellants were "not concerned of having the invention implemented in a network concept of socket as disclosed in the claims." This is simply not the case. As the Examiner acknowledges himself, p. 11, line 22 through p. 12 line 25 describe the use of sockets, and do so in a manner consistent with the claims.

Next, the Examiner states "[t]he plurality of sockets claimed by the applicant in the last action, as interpreted by the Examiner, represented the socket of the first connection and the matching socket." It is unclear from the Examiner's statement why he came to this conclusion. Claim 107 states:

> providing a plurality of sockets, wherein each socket has an associated connection and an associated security token, and the associated security token is provided by the associated connection;
>
> receiving a first connection and a first security token;
>
> creating a socket associated with the first connection, wherein the first connection has associated the first security token;
>
> comparing the first security token with the associated security tokens;
>
> in response to said comparing, if none of the associated security tokens match the first security token, including the socket in the plurality of sockets.

Thus, it is clear from claim 107 that "the first connection" is received, it has a first security token, and a socket associated with the first connection is created. That socket is included in "the plurality of sockets" that are provided when certain conditions are met, i.e., "in response to said comparing," and "if none of the associated security tokens match the first security token." Accordingly, the Examiner inaccurately characterizes the claim when he states "[t]he plurality of sockets . . . represented the socket."

Next, the Examiner states: "[g]iven the claims now as amended, it appears that Applicant is referring to the list of currently open sockets (to be searched for match), because Applicant now claims that the socket (interpreted as the attempted connection) is included in the plurality of sockets in response to no match." Again, the claimed "the socket" is only included in "the plurality of sockets" when certain conditions are met. Since the claim does not recite "currently open sockets," the appellants are not explicitly referring to that list in the claim. However, the description associated with the list of currently open sockets (e.g., p. 12, lines 1-3 and lines 12-14) does provide ample written description for the claimed "providing a plurality of sockets." The Examiner also "interprets" the claimed "the socket" as "the attempted connection." While the appellants have no particular opinion as to whether or not this interpretation is correct, they do respectfully submit there is ample written description supporting "the socket" and more particularly, "creating a socket . . . ," and "including the socket . . . ." For example, p. 11, lines 22-24 state:

> The exemplary process of Fig. 4 begins with the creation of a socket (step 400) for use by an in-bound connection.

Page 12, lines 17-19 state:

> If the attempted connection is to be configured as a listening connection, the attempted connection is put on the list of currently open sockets (step 470).

Clearly, since the connection is associated with a socket, and the connection is described as being added to the list of open sockets, there is ample support for the claimed "including the socket . . . ."

The Examiner goes on to state "[t]herefore, the specification does not describe, 'providing a plurality of sockets, wherein each socket has an associated connection and an associated security token and the associated security token is provided by the associated connection'." As demonstrated above, this conclusion is incorrect.

Next the Examiner argues, "[t]he disclosure does not even explicitly states, 'the socket' is included in the plurality of sockets." The mere fact that the claim term is not explicitly in the specification does not cause the claims to fail to comply with §112, first paragraph. This is emphasized by, for example, MPEP §2163(I)(B) which states in relevant part; "While there is no *in haec verba* requirement, newly added claim limitations must be supported in the specification through express, implicit, or inherent disclosure." So long as the disclosure reasonably conveys to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention, the written description requirement is satisfied. As demonstrated above, the appellants have also satisfied the requirement with respect to this limitation.

Next, the Examiner states "[i]n addition, the disclosure does not describe, 'creating a socket associated with the first connection wherein the first connection has associated the first security token.'" As noted above, socket creation is clearly supported by the specification. That connections can have associated security tokens is supported, for example, on p. 12, lines 1-7:

> Upon the receipt of an in-bound connection requisition (step 410), a list of currently open sockets maintained by relay program 210 is searched in an effort to locate an open socket having a matching password (step 420). It will be noted that the process illustrated in Fig. 4 is one that uses passwords for each connection in order to provide enhanced security. Although passwords need not be employed, some method of determining which in-bound connections are to be coupled to other in-bound connections should be supported by relay program 210.

Thus, sockets and/or connections have associated security tokens, e.g., passwords. The Examiner's elaboration: "[t]he disclosure merely states 'create a socket for use by an inbound connection' this socket was never mentioned afterwards, and merely states 'a password is provided,'" is also incorrect. The specification clearly describes more than creating a socket for use by an inbound connection.

Finally, the Examiner argues "[t]he association that Applicant is claiming with the created socket having an associated connection and associated token is not explicitly disclosed." Again, the appellants respectfully submit there is no requirement of explicit disclosure. So long as the disclosure reasonably conveys to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention, the written description requirement is satisfied. As noted above, there is ample support for sockets having an associated connection, and for connections having an associated security token.

In his Final Office Action of June 26, 2006, the Examiner provides some additional remarks. See, e.g., p. 3 and 4.

First, the Examiner states: "[t]here is no security token that is provided by each socket of the plurality of sockets as claimed." The appellants respectfully submit that the

Examiner has mischaracterized their claims. None of the rejected claims requires a socket to provide a security token.

Next, the Examiner states:

> Applicant states, that application further describes the password as being provided (application p.12:12). It is noted that this passage merely states "if the password provided"; applicant clarifies that it is the password provided by the attempted connection; therefore, it cannot be the password of the currently open sockets as recited in the claim.

The appellants are unable to ascertain the precise meaning of the Examiner's argument, and request clarification.

Next the Examiner notes that "the specification does not describe and specific association . . ." and that certain limitations are not explicitly shown. The appellants respectfully submit both the referenced limitations and the claimed association among security tokens, connections, and sockets, are described with sufficient detail for one having ordinary skill in the art.

Further regarding the "comparing the first security token . . . ," the Examiner makes a variety of statements concluding with:

> The passage "if a password matches a currently open socket..." does not explicitly describe comparing passwords with passwords of current open sockets.

However, the appellants respectfully submit that one having ordinary skill in the art would read the referenced passage (p. 12, lines 12-14) along with p. 12, lines 1-3 ("Upon the receipt of an in-bound connection requisition (step 410), a list of currently open sockets maintained by relay program 210 is searched in an effort to locate an open socket having a matching password (step 420)") and find adequate support for the claim limitation.

Next, the Examiner states:

> The claim limitation "including the socket in the plurality of sockets" does not equate "the attempted connection is put on the list of currently open sockets from the specification", and contrarily to applicant's assertion, there is nowhere in the specification it is disclosed that an attempted connection is associated with its own socket.

Whether or not the two quoted phrases "equate" is not the issue. At issue is whether the claim limitation finds adequate support (explicit or otherwise) in the specification. As noted above, the appellants submit there is ample support.

In summary, pp. 11 and 12, as well as Figure 4 provide adequate support for the claim limitations at issue. Accordingly, the appellants respectfully submit claims 107-119, 131-139, and 165-173 satisfy the requirements of 35 U.S.C. § 112, first paragraph.

35 U.S.C. § 112, First Paragraph – Claims 125-127, 145-147, and 179-181

Claims 125, 145, and 179 are explicitly rejected under 35 U.S.C §112, first paragraph. The claims depending from those claims also appear to be similarly rejected. *See* Final Office Action of June 26, 2006, p. 5, ¶1. The appellants present an argument with respect to claim 125, as the relevant limitations in independent claims 145 and 179 are generally the same as those in claim 125. Further, claims 126-127, 146-147, and 180-181 depend from claims 125, 145, and 179, respectively.

To the extent these claims are rejected for the same reasons as claims 107-119, 131-139, and 165-173, the appellants refer to the arguments set out above. Additionally, the Examiner states:

> Not even the amended claims 125 and 145 reciting, in response to the comparing if there is no match, including the second connection with said one or more corresponding connections, was not described in the specification as explained above as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. (Final Office Action of June 26, 2006, p. 6, top)

The appellants respectfully disagree. Claim 125 requires "in response to said comparing, if none of the associated security tokens match the first security token, including the second connection with said one or more corresponding connections."

The appellants respectfully submit there is ample written description supporting "including the second connection . . . ." For example, p. 11, lines 22-24 state:

> The exemplary process of Fig. 4 begins with the creation of a socket (step 400) for use by an in-bound connection.

Page 12, lines 17-19 state:

> If the attempted connection is to be configured as a listening connection, the attempted connection is put on the list of currently open sockets (step 470).

Clearly, since sockets are associated with connections, and the connection is described as being added to the list of open sockets, there is ample support for the claimed "including the second connection with said one or more corresponding connections."

Accordingly, the appellants respectfully submit claims 125-127, 145-147, and 179-181 satisfy the requirements of 35 U.S.C. § 112, first paragraph.

35 U.S.C. § 102(e) Rejection – Claims 107-119, 131-139, and 165-173

Claims 107-119, 131-139, and 165-173 stand rejected under 35 U.S.C. § 102(e) (either directly or via a rejected parent claim) as being anticipated by U. S. Patent 5,941,988 issued to Bhagwat. The appellants present an argument with respect to independent claim 107, as the relevant limitations in independent claims 131 and 165 are generally the same as those in claim 107. Further, claims 108-119, 132-139, and 166-173 depend from independent claims 107, 131, and 165, respectively.

Bhagwat fails to teach or suggest a method including:

> . . . comparing the first security token with the associated security tokens;
>
> in response to said comparing, if none of the associated security tokens match the first security token, including the socket in the plurality of sockets.

as required by independent claim 107, and generally required by independent claims 131 and 165.

Regarding the claimed "comparing the first security token with the associated security tokens," the Examiner states: "**Bhagwat et al** also discloses creating a socket associated with the first connection (column 7, lines 13-26) and an authentication test that meets the recitation of comparing the first security token with the associated security tokens (column 7, lines 13-26; column 5, lines 1-20 see also column 8, lines 1-8)." Final Office Action of June 26, 2006, p. 8, top, emphasis original. The cited portions of Bhagwat state (in column order):

> . . . from the server, not the proxy. As shown in FIG. 2, the client's designer can use the OK message for synchronization by opening a connection to the server, exchanging session set up data with the proxy, and then blocking until the OK message arrives.
>
> In the message exchange illustrated in FIG. 2 between a Telnet client 11, a proxy firewall 12 and a Telnet server 13, the Telnet client 11 opens the connection and sets up the connection by transmitting the server address to the firewall proxy 12. In response to an authentication challenge from the firewall proxy 12, the Telnet client 11 provides an authentication reply. The TCP glue 14 is then set up by the firewall proxy 12, and while this occurs, the Telnet client 11 blocks further communication. When the TCP glue is set up, a connection is opened with the Telnet server 13 and an OK message is sent to the Telnet client 11. Upon receipt of the OK message,

> communication is unblocked and data1 from the Telnet client 11 is transmitted to the Telnet server 13 via the firewall proxy 12 and data2 from the Telnet server 13 is transmitted to the Telnet client via the firewall proxy 12.
>
> . . .
>
> At the proxy, socket A stays in the LISTEN state 51 until it receives an "OPEN CONNECTION" message (called SYN packet in TCP terminology) from the client or local host. The proxy replies with a SYN & ACK message and moves to the SYN_RCVD state 52. When the acknowledgment for SYN & ACK arrives from the client, the connection between the client and the proxy is established at state 53. Over the newly established connection, using SOCKS version 4 or 5 protocol, the client and the proxy exchange authentication information. If the client fails the authentication test, socket A returns to LISTEN state 51, resetting the connection between the client and the proxy. Upon the successful completion of the authentication process, the connection moves to ESTABLISHED AND AUTH state 54.
>
> . . .
>
> Alter IP Header
> C Change source and destination address to that of outgoing connection.
> C Remove IP options from incoming packet.
> C Update IP header checksum.
> Alter TCP Header
> C Change source and destination port numbers to match outgoing connection.

The cited portion of column 5 generally discusses enabling synchronization using TCP. The cited portion of column 7 describes the establishment of a connection at socket A, and subsequent exchange of authentication information according to SOCKS. The cited portion of column 8 describes changes to various headers. None of these portions of Bhagwat teach or suggest comparing an address or port number, i.e., that which the Examiner equates with the claimed security token, with *anything*.

The Examiner separately refers to the use of username/password authentication in SOCKS as also teaching the claimed security tokens. However, the Examiner fails to point out any portion of Bhagwat teaching or suggesting comparison of a SOCKS authentication username or password with anything corresponding to "the associated security tokens," i.e., security tokens corresponding to respective ones of the recited plurality of sockets. The cited portion of column 7 merely states "the client and the proxy exchange authentication information." The referenced SOCKS authentication merely describes authentication by a server of a username and password provided by a client. At best, and the appellants do not concede this point, this suggests comparing the username/password supplied by the client with that stored on the server. It does not, however, teach or suggest comparing a first security token with the associated security tokens of *other sockets.*

The Examiner goes on to argue:

> **Bhagwat et al** also discloses checking the authentication test (column 7, lines 12-25) and discloses a mapping process that includes comparing the security token of the client to associated security tokens also discloses matching port numbers or addresses that meets the recitation of comparing the first security token with the associated security tokens, for example (column 6, lines 35-43; and column 7, line 55 through column 8, line 24; see also column 4, lines 22-37); **Bhagwat et al** further discloses ion one embodiment that if authentication fails the socket returns to listen state as an open connection that meets the recitation of including the socket in the plurality of sockets (column 7, lines 13-56). (Final Office Action of June 26, 2006, p. 8, top, emphasis original)

The appellants respectfully disagree.

First, it is unclear precisely what the Examiner means by "checking the authentication test." Bhagwat does state "If the client fails the authentication test, socket A returns to LISTEN state 51," but this does not teach or suggest the claimed "comparing the first security token with the associated security tokens," or "including the socket in the plurality of sockets."

Second, the Examiner references a "mapping process." Column 6, lines 35-43, column 7, line 55 through column 8, line 24; and column 4, lines 22-37 state (respectively):

> Mapping Sequence Numbers
> Since both connections (client-proxy and proxy-server) have their own sequence spaces, as segments arrive on one connection (say, the proxy-server connection) all the sequence space related information must be mapped to the sequence space of the other connection (the client-proxy connection) before forwarding or the segment will not be intelligible to the other end-system (the client).

> Modifying Packet Headers
> As each segment is received at a glued socket, the segment's headers are altered to address the segment to the socket at the other end of the glued connection. The segment's TCP headers are altered so the segment will be intelligible to the end system when it arrives; that is, the segment will look like a continuation of the normal TCP connection the end system first started with the proxy. Processing a segment requires three steps; changing the IP and TCP headers and making special sanity checks.
> Alter IP Header
> C Change source and destination address to that of outgoing connection.
> C Remove IP options from incoming packet.
> C Update IP header checksum.
> Alter TCP Header
> C Change source and destination port numbers to match outgoing connection.
> C Map sequence number from incoming sequence space to outgoing space. seq_num=(seq_num-in6glue_irs) +out6glue_iss
> C Map ACK number from incoming sequence space to outgoing space. ack_num=(ack_num-in6glue_iss) +out6glue_irs
> C Update TCP header checksum.
> Perform Sanity Checks
> The OK message marks the boundary between the client communicating with the proxy and the client communicating with the server. Any reference the client makes to sequence numbers before the mapping points (A glue_iss in FIG. 4) must be processed by the proxy's normal TCP state machine since the client could be requesting retransmissions of the OK message or other complicated functionality.
>
> TCP connections also have state in the form of TCP options negotiated at connection setup time. In the preferred embodiment of the invention, the TCP glue does not ensure that the same options are negotiated on both the proxy-client and proxy-server connections, so it is possible these connections will be negotiated with different TCP options. This could create problems once the two connections are glued together, since an end system may receive TCP options that it does not expect or have options it expects to be processed by the other end system. If options mismatch does create a problem, the preferred embodiment of the invention could be modified with the addition of a new kernel call to the proxy networking stack to negotiate the same set of options when connecting a new socket as were negotiated on an existing socket.

These disparate portions of Bhagwat discuss mapping sequence space, packet modification, sanity checks, and TCP setup. However, none of them teach or suggest either the claimed "comparing the first security token with the associated security tokens," or "including the socket in the plurality of sockets." Moreover, the Examiner provides no guidance as to why these portions of Bhagwat purportedly teach the claim limitations.

Finally, the Examiner merely concludes that Bhagwat's returning to LISTEN state 51 if the client fails the authentication test, teaches the claimed "plurality of sockets, wherein each socket has an associated connection and an associated security token, and the associated security token is provided by the associated connection." This cannot be the case because, at a minimum, Bhagwat's LISTEN state simply resets the same connection between client and proxy for another authentication attempt, i.e., it does not teach or suggest a plurality of provided sockets.

MPEP §2131 makes clear the requirements for anticipation:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). . . . "The identical invention must be shown in as complete detail as is contained in the . . . claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). (Emphasis added)

Thus, in addition to showing every element, the reference must teach their arrangement as required by the claim. The Examiner has failed to demonstrate that Bhagwat teaches all of the claim limitations, and those things the Examiner does point to in Bhagwat are not arranged as required by the claim.

The appellants note that the Examiner provides additional argument with respect to Bhagwat (Final Office Action of June 26, 2006, p. 4, ¶2), but submit the further reference to "two independent connections" and column 7 lines 20-36, fail to demonstrate either the "comparing the first security token with the associated security tokens," or "including the socket in the plurality of sockets."

Accordingly, the appellants respectfully submit independent claims 107, 131, and 165 are allowable over Bhagwat. Further, claims 108-119, 132-139, and 166-173 depend from independent claims 107, 131, and 165, respectively, and are allowable for at least this reason.

35 U.S.C. § 102(e) Rejection – Claims 120-130, 140-147, and 174-181

Claims 120-130, 140-147, and 174-181 stand rejected under 35 U.S.C. § 102(e) (either directly or via a rejected parent claim) as being anticipated by U. S. Patent 5,941,988 issued to Bhagwat. The appellants present an argument with respect to independent claim 120, as the relevant limitations in independent claims 140 and 174 are generally the same as those in claim 120. Further, claims 121-130, 141-147, and 175-181 depend from independent claims 120, 140, and 174, respectively.

Bhagwat fails to teach or suggest a method including:

> . . . receiving a first security token from the first program;
>
> . . . providing the first security token to the relay program; and
>
> upon successful creation of the second connection, coupling the first connection to the second connection,

as required by independent claim 120, and generally required by independent claims 140 and 170.

The Examiner's arguments are outlined at Final Office Action of June 26, 2006, p. 10, bottom, through p. 11, top. In general, the Examiner refers to column 5, lines 5-20:

> In the message exchange illustrated in FIG. 2 between a Telnet client 11, a proxy firewall 12 and a Telnet server 13, the Telnet client 11 opens the connection and sets up the connection by transmitting the server address to the firewall proxy 12. In response to an authentication challenge from the firewall proxy 12, the Telnet client 11 provides an authentication reply. The TCP glue 14 is then set up by the firewall proxy 12, and while this occurs, the Telnet client 11 blocks further communication. When the TCP glue is set up, a connection is opened with the Telnet server 13 and an OK message is sent to the Telnet client 11. Upon receipt of the OK message, communication is unblocked and data1 from the Telnet client 11 is transmitted to the Telnet server 13 via the firewall proxy 12 and data2 from the Telnet server 13 is transmitted to the Telnet client via the firewall proxy 12.

The Examiner equates the claimed first program with proxy 12, the claimed relay program with server 13, and regarding the claimed "receiving a first security token from the first program," refers to the lines 18-20 ("Upon receipt of the OK message, communication is unblocked and data1 from the Telnet client 11 is transmitted to the Telnet server 13 via the firewall proxy 12 . . . .") First, the Examiner provides no justification for the conclusion that "data1" is necessarily a security token. Second, "data1" is only transmitted to server 13 (i.e., that which the Examiner equates with the claimed relay program) once the two connections (client-to-proxy and proxy-to-server) are joined. Consequently, the "upon successful creation of the second connection, coupling the first connection to the second connection" limitation is not satisfied by Bhagwat because Bhagwat teaches coupling the connections *before* data1 can be transmitted to server 13. Finally, server 13 is not a relay program within the meaning of the term as used in appellant's specification and as would be understood to those skilled in the art.

Accordingly, independent claims 120, 140, and 174 are allowable over Bhagwat. Further, claims 121-130, 141-147, and 175-181 depend from independent claims 120, 140, and 174, respectively and are allowable for at least this reason.

CONCLUSION

The appellants respectfully submit claims 107-147 and 165-181 are allowable over Bhagwat and satisfy the requirements of 35 U.S.C. § 112, first paragraph. For at least the reasons stated above, claims 107-147 and 165-181 are allowable. The appellants respectfully request that the Board reverse the rejections of these claims.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA, 22313-1450, on Nov 27, 2006.

	11/27/06
Attorney for Appellant(s)	Date of Signature

Respectfully submitted,

Marc R. Ascolese
Attorney for Appellant
Reg. No. 42,268
512-439-5085
512-439-5099 (fax)

CLAIMS APPENDIX

107. A method comprising:

providing a plurality of sockets, wherein

each socket has an associated connection and an associated security token, and

the associated security token is provided by the associated connection;

receiving a first connection and a first security token;

creating a socket associated with the first connection, wherein

the first connection has associated the first security token;

comparing the first security token with the associated security tokens;

in response to said comparing, if none of the associated security tokens match the first security token, including the socket in the plurality of sockets.

108. The method of Claim 107, wherein

a security token is one of a password, a network address, and a verification string.

109. The method of Claim 107 further comprising:

in response to said comparing, if the first security token and a security token associated with one of the plurality of sockets match, coupling the first connection to the connection associated with the socket associated with the matching security token.

110. The method of Claim 107 further comprising:

in response to said comparing, if none of the associated security tokens match the first security token,

upon a determination that the first connection is not to be associated with a socket, disconnecting the first connection.

111. The method of Claim 109, wherein the coupling the first connection to the connection associated with the socket comprises:

relaying a data stream between the first connection and the connection associated with the socket.

112. The method of Claim 109, wherein the coupling the first connection to the connection associated with the socket comprises:

creating a single connection comprising the first connection and the connection associated with the socket.

113. The method of Claim 109 further comprising:

decoupling the first connection and the connection associated with the socket.

114. The method of Claim 113, wherein

the decoupling occurs upon one of failure and disconnect of one of the first connection and the connection associated with the socket.

115. The method of Claim 109, wherein

the first connection is transmitted through a first firewall program.

116. The method of Claim 115, wherein

the first connection is created by a protocol daemon.

117. The method of Claim 116, wherein

a second connection connects the protocol daemon to a first program, and

the protocol daemon couples the first connection to the second connection.

118. The method of Claim 117, wherein

the protocol daemon relays a data stream between the first connection and the second connection.

119. The method of Claim 118, wherein
the first program provides the first security token.

120. A method comprising:
creating a first connection to a first program;
receiving a first security token from the first program;
creating a second connection to a relay program;
providing the first security token to the relay program; and
upon successful creation of the second connection, coupling the first connection to the second connection.

121. The method of Claim 120, wherein
the second connection is transmitted through a firewall program.

122. The method of Claim 120 further comprising:
relaying a data stream between the first connection and the second connection.

123. The method of Claim 120, wherein
the first security token is one of a password, a network address, and a verification string.

124. The method of Claim 120 further comprising:
terminating the first connection and the second connection.

125. The method of Claim 120, wherein
the relay program compares the first security token with one or more security tokens associated with one or more corresponding connections;
in response to said comparing, if the first security token and a security token associated with a corresponding connection match,
coupling the second connection to the connection associated with the matching security token; and

in response to said comparing, if none of the associated security tokens match the first security token,

including the second connection with said one or more corresponding connections.

126. The method of Claim 125, wherein

the connection associated with the matching security token is initiated by a second program.

127. The method of Claim 125, wherein

the relay program relays data between the second connection and the connection associated with the matching security token.

128. The method of Claim 121, wherein

a protocol daemon program does the creating the first connection, the creating the second connection, the receiving the first security token from the first program, the providing the first security token to the relay program, and the coupling the first connection to the second connection.

129. The method of Claim 128, wherein

the protocol daemon program and the firewall program are resident on a single computer.

130. The method of Claim 128, wherein

the protocol daemon program and the first program are resident on a single computer.

131. An apparatus comprising:

means for providing a plurality of sockets, wherein

each socket has an associated connection and an associated security token, and

the associated security token is provided by the associated connection;

means for receiving a first connection and a first security token;

means for creating a socket associated with the first connection, wherein the first connection has associated the first security token;

means for comparing the first security token with the associated security tokens;

in response to said comparing, if none of the associated security tokens match the first security token, means for including the socket in the plurality of sockets.

132. The apparatus of Claim 131, wherein

a security token is one of a password, a network address, and a verification string.

133. The apparatus of Claim 131 further comprising:

in response to said comparing, if the first security token and a security token associated with one of the plurality of sockets match, means for coupling the first connection to the connection associated with the socket associated with the matching security token.

134. The apparatus of Claim 131 further comprising:

in response to said comparing, if none of the associated security tokens match the first security token,

upon a determination that the first connection is not to be associated with a socket, means for disconnecting the first connection.

135. The apparatus of Claim 133, wherein the means for coupling the first connection to the connection associated with the socket comprises:

means for relaying a data stream between the first connection and the connection associated with the socket.

136. The apparatus of Claim 133, wherein the means for coupling the first connection to the connection associated with the socket comprises:

means for creating a single connection comprising the first connection and the connection associated with the socket.

137. The apparatus of Claim 133 further comprising:
means for decoupling the first connection and the connection associated with the socket.

138. The apparatus of Claim 137, wherein
the decoupling occurs upon one of failure and disconnect of one of the first connection and the connection associated with the socket.

139. The apparatus of Claim 133, wherein
the first connection is transmitted through a first firewall program.

140. An apparatus comprising:
means for creating a first connection to a first program;
means for receiving a first security token from the first program;
means for creating a second connection to a relay program;
means for providing the first security token to the relay program; and
means for coupling the first connection to the second connection upon successful creation of the second connection.

141. The apparatus of Claim 140 further comprising
means for transmitting the second connection through a firewall program.

142. The apparatus of Claim 140 further comprising:
means for relaying a data stream between the first connection and the second connection.

143. The apparatus of Claim 140, wherein
the first security token is one of a password, a network address, and a verification string.

144. The apparatus of Claim 140 further comprising:
means for terminating the first connection and the second connection.

145. The apparatus of Claim 140, wherein the relay program further comprises:
means for comparing the first security token with one or more security tokens associated with one or more corresponding connections;
means for coupling the second connection to a connection associated with a security token, if the first security token and the security token associated with the corresponding connection match; and
means for including the second connection with said one or more corresponding connections, in response to ~~if~~ none of the security tokens associated with the one or more corresponding connections matching the first security token.

146. The apparatus of Claim 145, wherein
the connection associated with the matching security token is initiated by a second program.

147. The apparatus of Claim 145, wherein the relay program further comprises:
means for relaying data between the second connection and the connection associated with the matching security token.

165. A computer program product encoded in computer readable media, the computer program product comprising:
a first set of instructions, executable by a processor and configured to cause the processor to provide a plurality of sockets, wherein
each socket has an associated connection and an associated security token, and
the associated security token is provided by the associated connection;
a second set of instructions, executable by the processor and configured to cause the processor to receive a first connection and a first security token;

a third set of instructions, executable by the processor and configured to cause the processor to create a socket associated with the first connection, wherein the first connection has associated the first security token;

a fourth set of instructions, executable by the processor and configured to cause the processor to compare the first security token with the associated security tokens;

a fifth set of instructions, executable by the processor and configured to cause the processor to include the socket in the plurality of sockets, in response to said comparing, if none of the associated security tokens match the first security token.

166. The computer program product of Claim 165, wherein a security token is one of a password, a network address, and a verification string.

167. The computer program product of Claim 165 further comprising:

a sixth set of instructions, executable by the processor, responsive to said comparing, and configured to cause the processor to couple the first connection to the connection associated with the socket associated with the matching security token if the first security token and a security token associated with one of the plurality of sockets match.

168. The computer program product of Claim 165 further comprising:

a seventh set of instructions, executable by the processor, responsive to said comparing, and configured to cause the processor to disconnect the first connection,

if none of the associated security tokens match the first security token, and

upon a determination that the first connection is not to be associated with a socket.

169. The computer program product of Claim 167 further comprising:

an eighth set of instructions, executable by the processor and configured to cause the processor to relay a data stream between the first connection and the connection associated with the socket.

170. The computer program product of Claim 167 further comprising:

a ninth set of instructions, executable by the processor and configured to cause the processor to create a single connection comprising the first connection and the connection associated with the socket.

171. The computer program product of Claim 167 further comprising:

a tenth set of instructions, executable by the processor and configured to cause the processor to decouple the first connection and the connection associated with the socket.

172. The computer program product of Claim 171 further comprising:

an eleventh set of instructions, executable by the processor and configured to cause the processor to decouple the first connection and the connection associated with the socket upon one of failure and disconnect of one of the first connection and the connection associated with the socket.

173. The computer program product of Claim 167, wherein the first connection is transmitted through a first firewall program.

174. A computer program product encoded in computer readable media, the computer program product comprising:

a first set of instructions, executable by a first processor and configured to cause the first processor to create a first connection to a first program;

a second set of instructions, executable by the first processor and configured to cause the first processor to receive a first security token from the first program;

a third set of instructions, executable by the first processor and configured to cause the first processor to create a second connection to a relay program;

a fourth set of instructions, executable by the first processor and configured to cause the first processor to provide the first security token to the relay program; and

a fifth set of instructions, executable by the first processor and configured to cause the first processor to couple the first connection to the second connection upon successful creation of the second connection.

175. The computer program product of Claim 174, wherein the second connection is transmitted through a firewall program.

176. The computer program product of Claim 174 further comprising:

a sixth set of instructions, executable by the first processor and configured to cause the first processor to relay a data stream between the first connection and the second connection.

177. The computer program product of Claim 174, wherein the first security token is one of a password, a network address, and a verification string.

178. The computer program product of Claim 174 further comprising:

a seventh set of instructions, executable by the first processor and configured to cause the first processor to terminate the first connection and the second connection.

179. The computer program product of Claim 174, wherein the relay program comprises:

an eighth set of instructions, executable by a second processor and configured to cause the second processor to compare the first security token with one or more security tokens associated with one or more corresponding connections;

a ninth set of instructions, executable by the second processor, responsive to said comparing, and configured to cause the second processor to couple the second connection to the connection associated with the matching security token if the first security token and a security token associated with a corresponding connection match; and

a tenth set of instructions, executable by the second processor, responsive to said comparing, and configured to cause the second processor to include the second connection with said one or more corresponding connections if none of the associated security tokens match the first security token.

180. The computer program product of Claim 179, wherein the connection associated with the matching security token is initiated by a second program.

181. The computer program product of Claim 179, wherein the relay program further comprises:

an eleventh set of instructions, executable by the second processor, configured to cause the second processor to relay data between the second connection and the connection associated with the matching security token.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.